The Great Firewall of China is the Chinese government's internet censorship and surveillance project.

The firewall prohibits people inside China from accessing many websites including Google, Twitter, New York Times, Youtube, Github, Dropbox, Gmail, Netflix, Vimeo, Instagram, Soundcloud, Flickr, Android, Appledaily, various porn websites and so on.

This project allows the Chinese government to restrict content on the internet that it deems sensitive or harmful (e.g. Tiananmen event, Falun Gong, Tibet, the illegal sales of drug/gun/porn).

From a technical perspective,
how does the Great Firewall work?

There are three main methods:

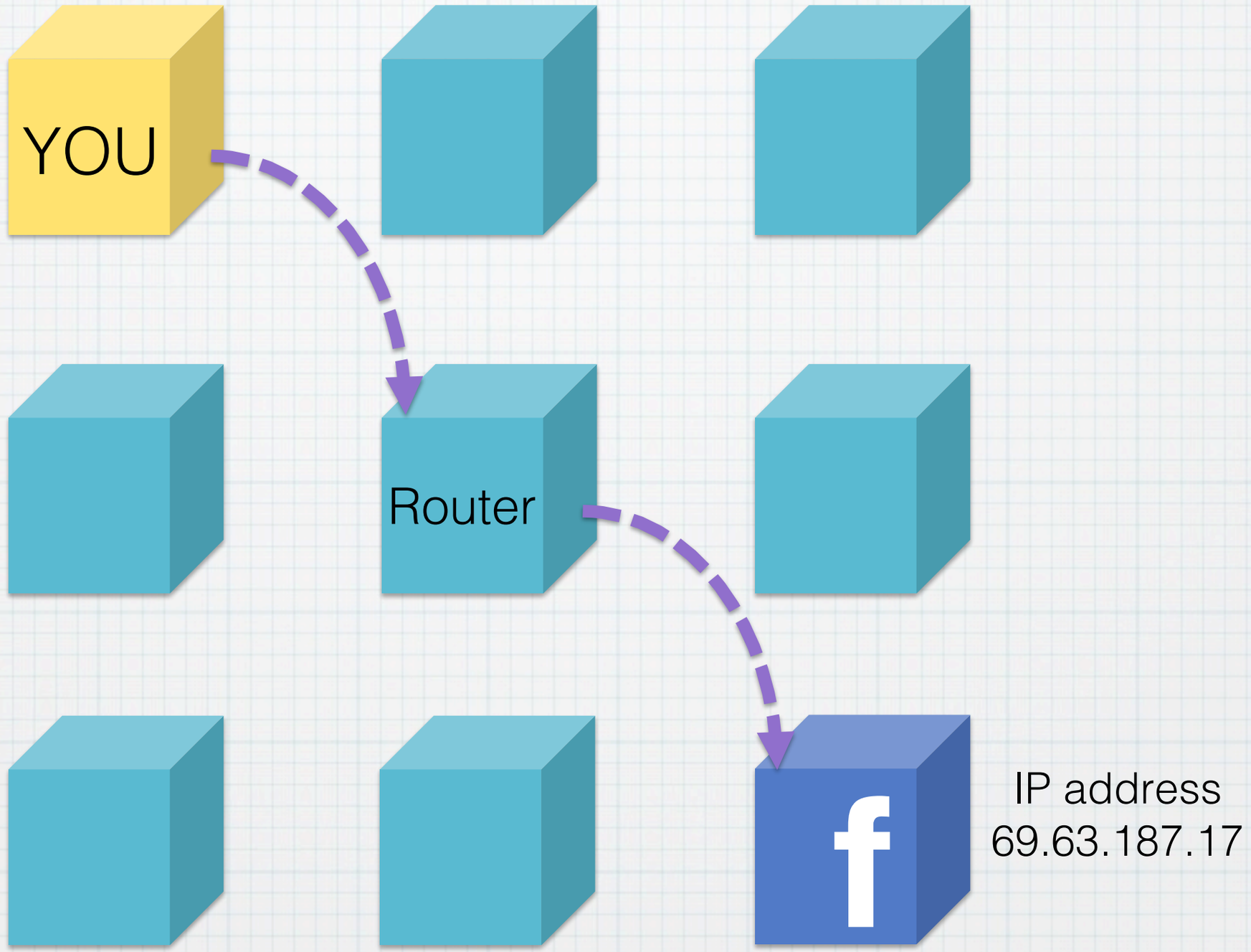
-IP Address Blocking

-DNS Hijacking

-Data Filtering: URL Filtering / Packet Filtering

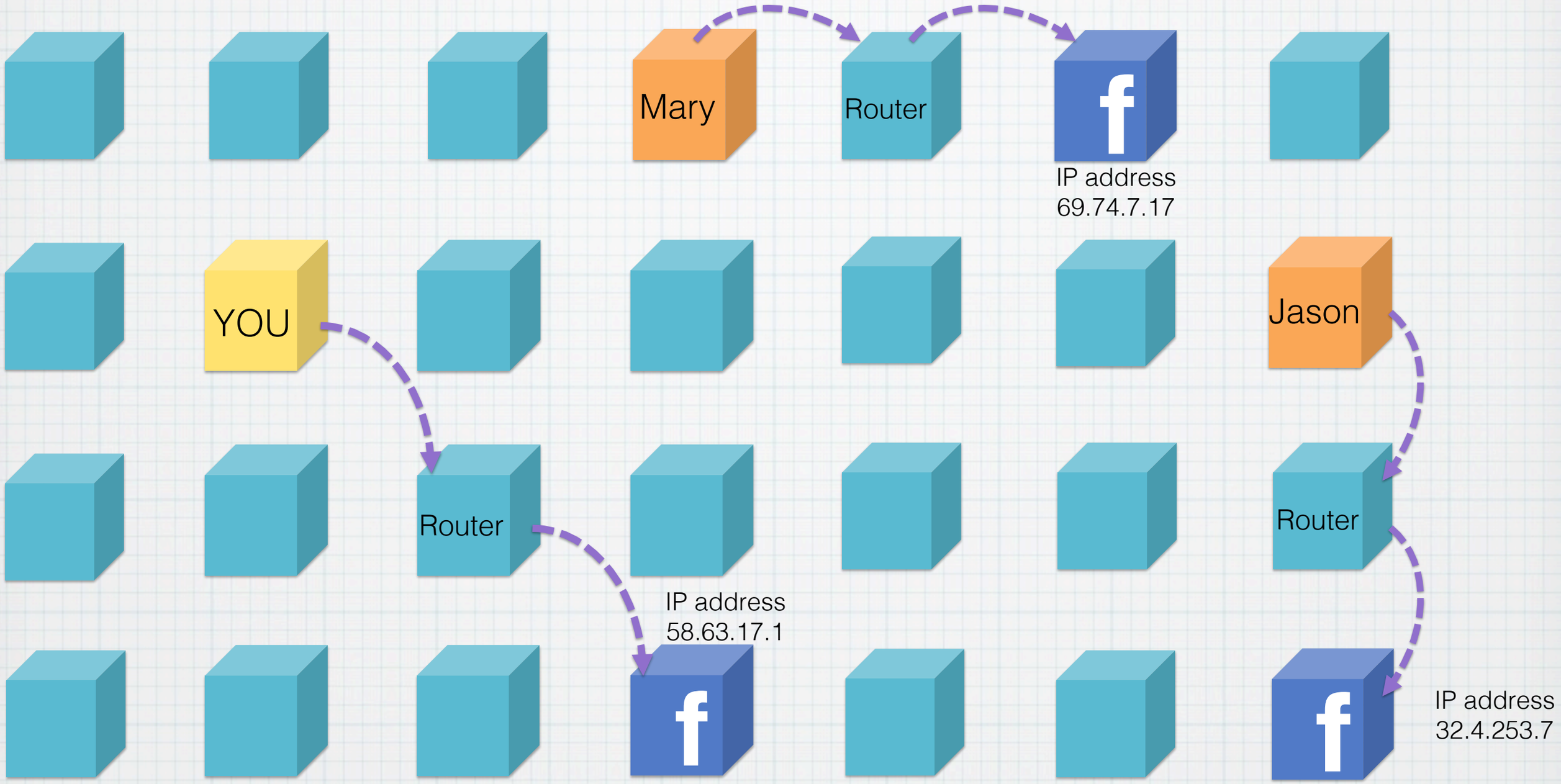
IP Address Blocking

The internet is basically a huge pile of computers. Each time you go to facebook.com, you're establishing a connection with that computer. The remote computer sends you some data, which you can view via your browser.



Every machine on the Internet has a unique numerical address, called an Internet Protocol (IP) address, used to route packets to it across the Internet.

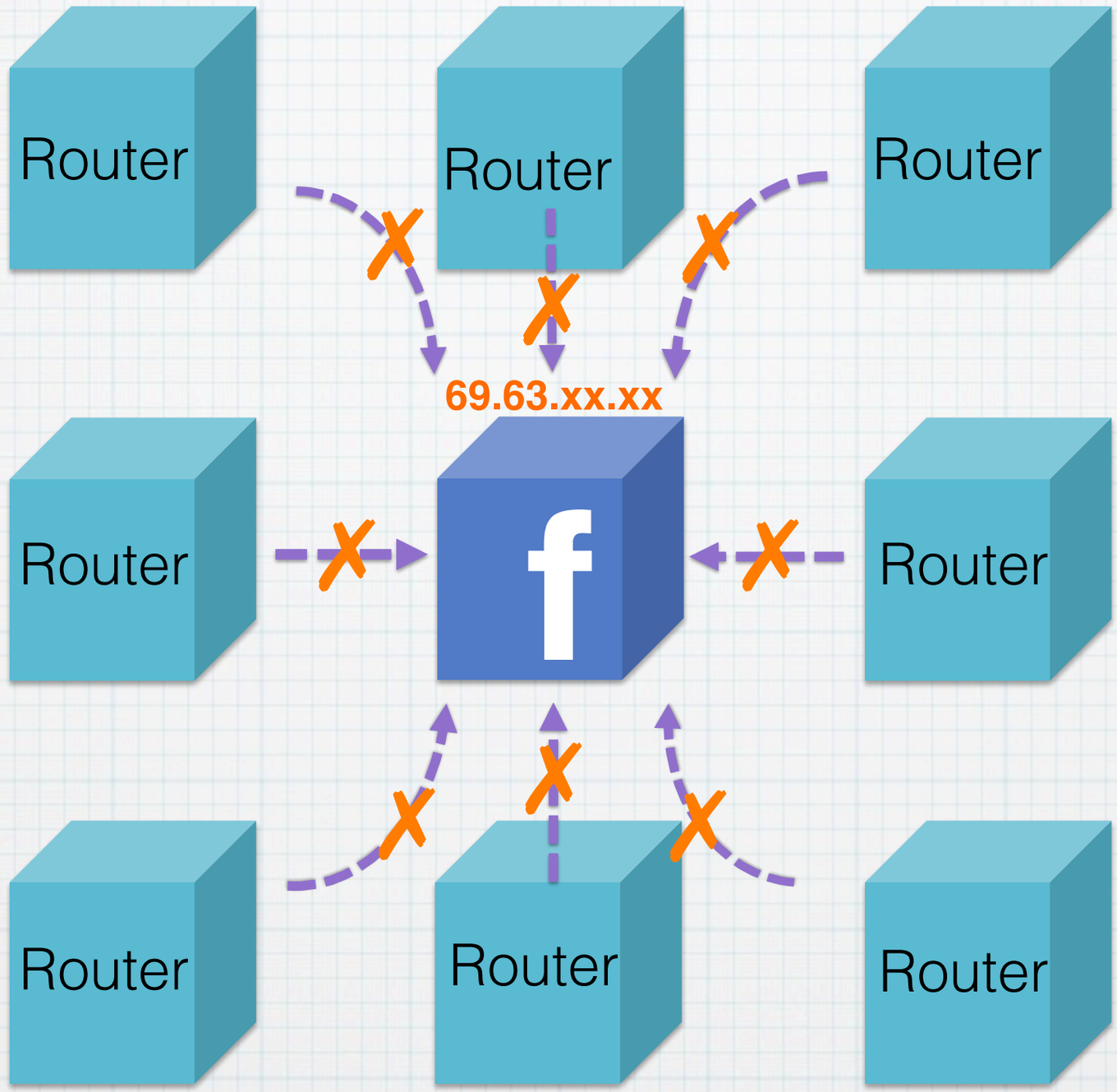
Why do we need to know the IP address every time we visit a website?



When you go to your facebook.com, you may not be going to the same computer. Depending on where it might be more convenient for you to go to a computer that's closer to where you are. If you were shopping for your groceries, you would go to a different convenience store depending on where you lived. So, the grocery store is better identified by it's address, rather than it's name. There are many Ralph's all over the country, but there is only one a block away from your home. Computers are much the same way. Different machine on the Internet may go to different computers to visit the same website depending on their locations. We need to know the IP address every time we visit a website.

*** Note: big companies like Facebook, Microsoft have hundreds of thousands of severs around the world.

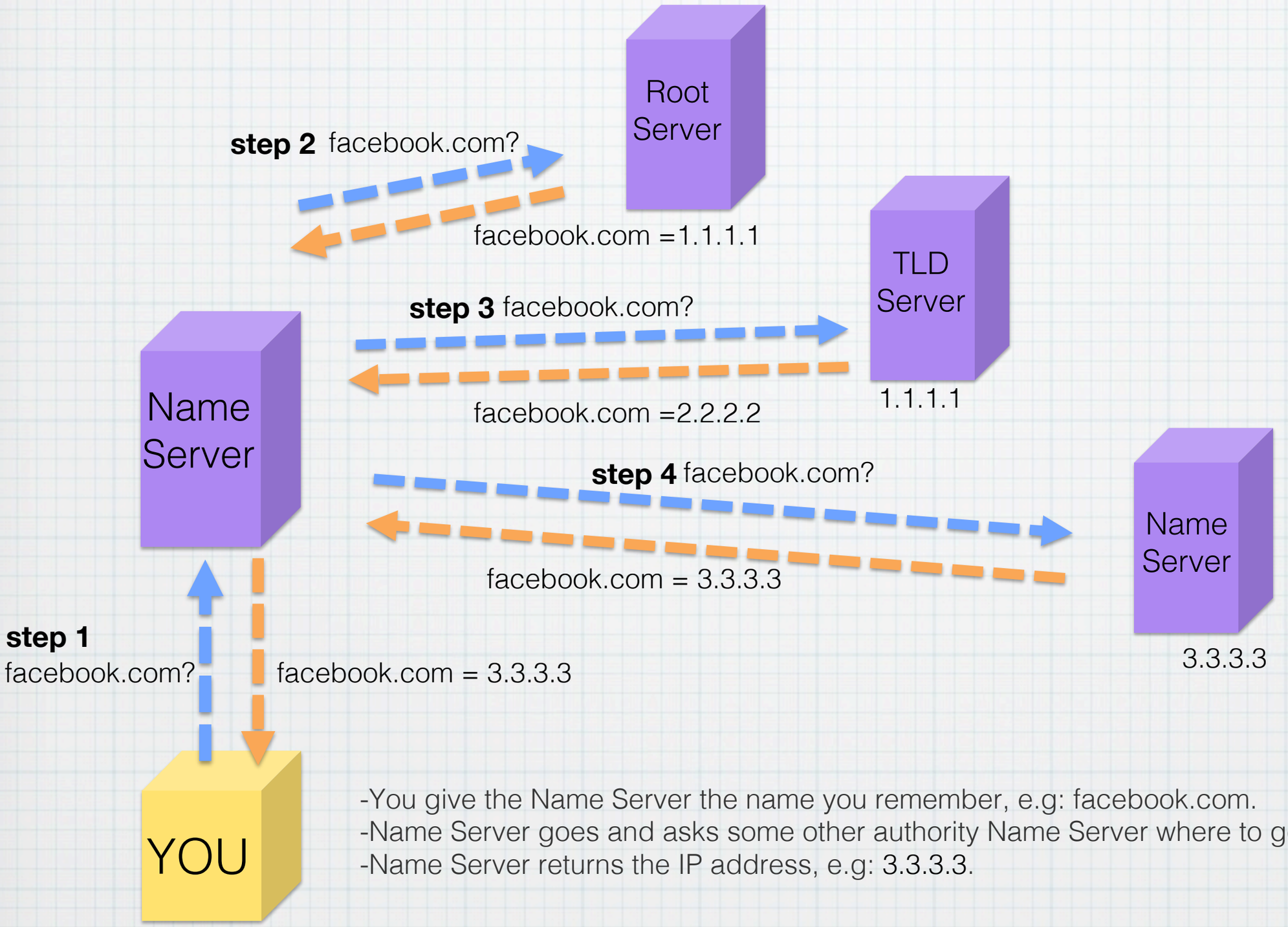
IP Address Blocking



Every Website uses at least one numeric address. Blocking this IP address prevents access to that individual site. Traffic to blocked IP addresses is dropped by the router. For example: facebook.com maps to a known IP address (e.g 69.63.xx.xx) so any connection made to that location is disconnected by the firewall.

DNS Hijacking

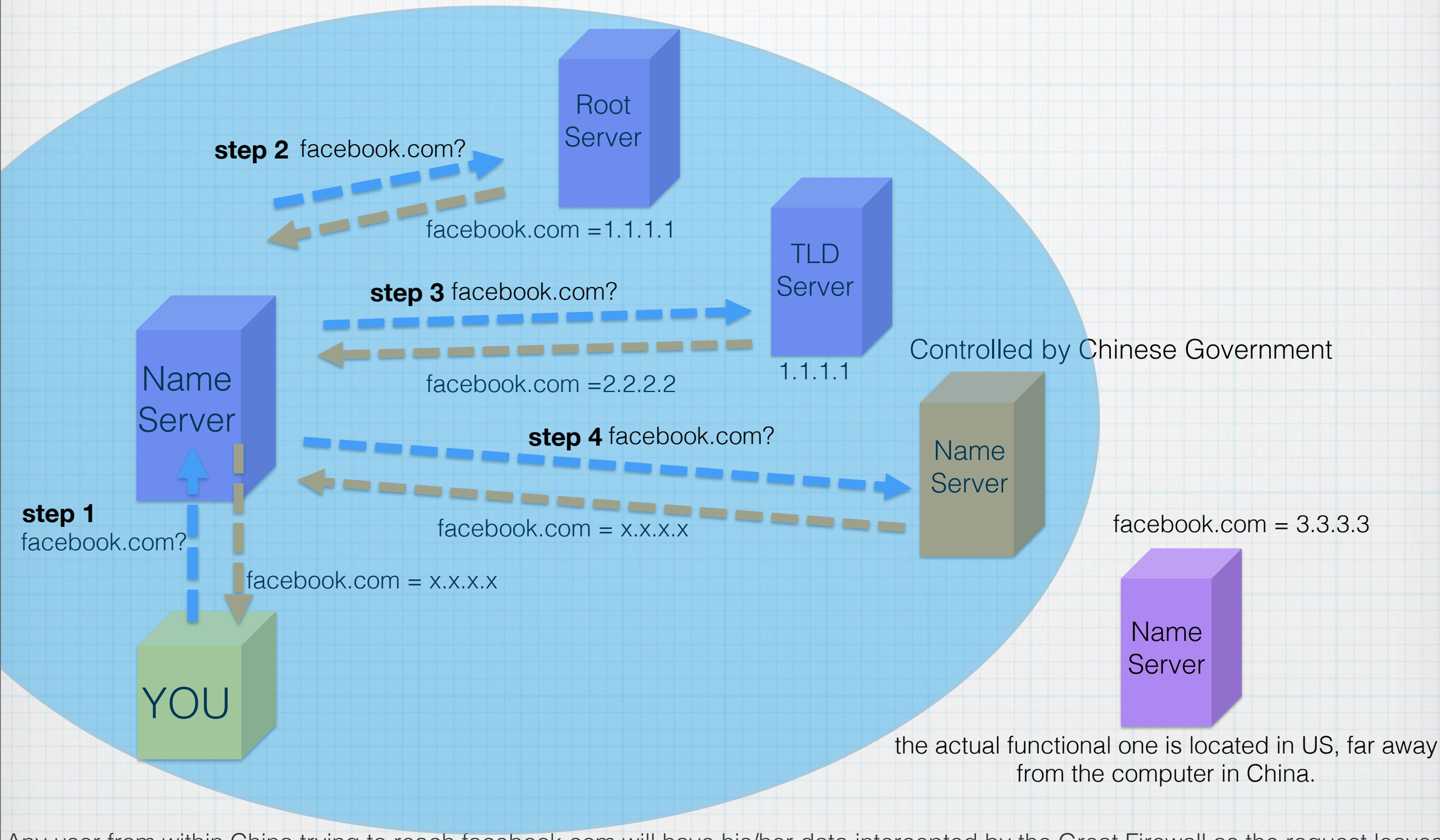
IP addresses are very hard to remember. So instead of using IP addresses to navigate to the computers we want, we tend to use human readable domain names, like facebook.com. The side effect to doing this is that each time we want to go to the domain name we remember we must go look up the IP address before we can connect and fetch the data we want. The machine for this is called a Name server.



-You give the Name Server the name you remember, e.g: facebook.com.
-Name Server goes and asks some other authority Name Server where to go.
-Name Server returns the IP address, e.g: 3.3.3.3.

***Note: every name server must depend on an authority name server, and trust falls completely on the authority name server.

The Internet must basically trust all authoritative name servers to give it the correct IP addresses for a given name. However, the Chinese government controls the majority of the internet presence and many of the authoritative name servers. By exploiting a flaw in the naming system, the name system will not resolve domain names, and return empty or incorrect IP addresses.



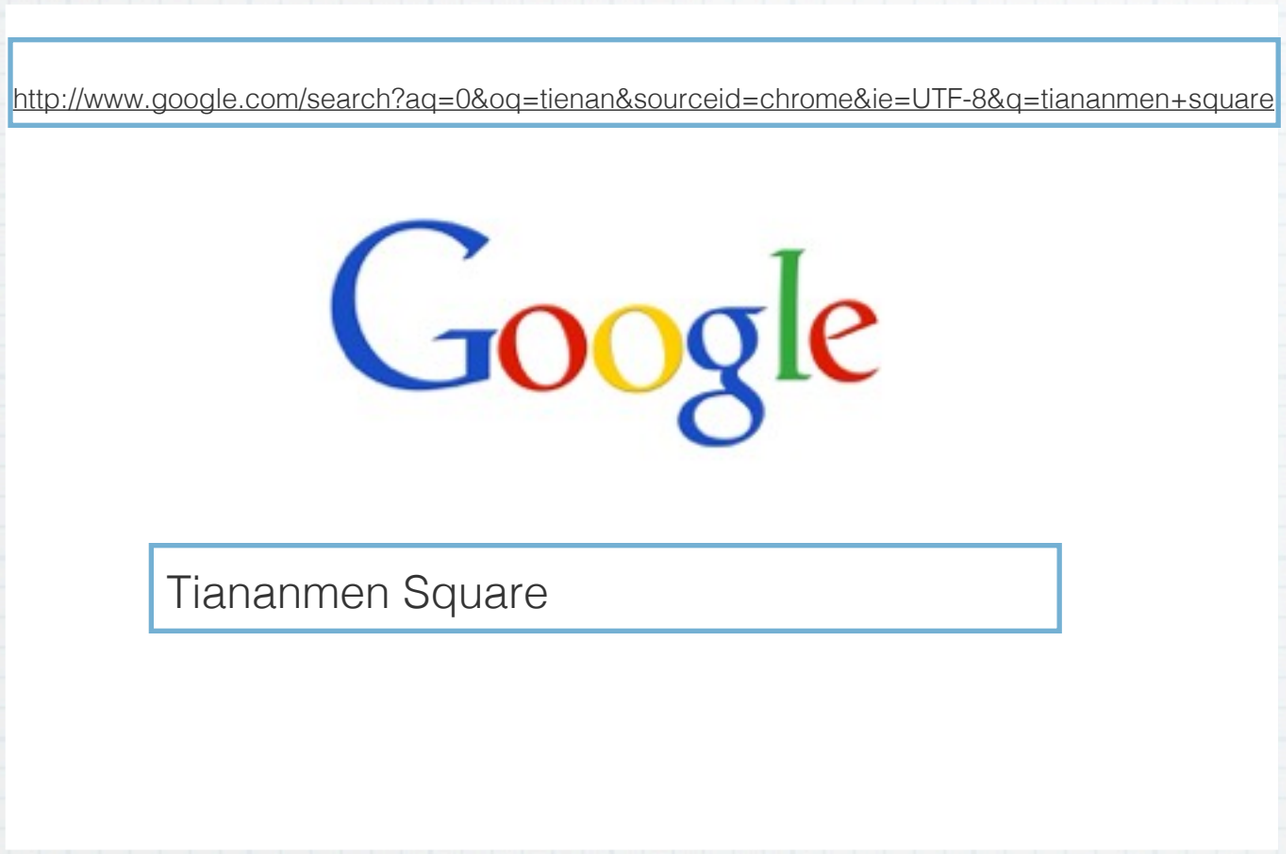
Any user from within China trying to reach facebook.com will have his/her data intercepted by the Great Firewall as the request leaves China. Then, before Facebook(which is located on the other side of the world) even sees the request, the Chinese government will issue a fake response to the original request solicitor.

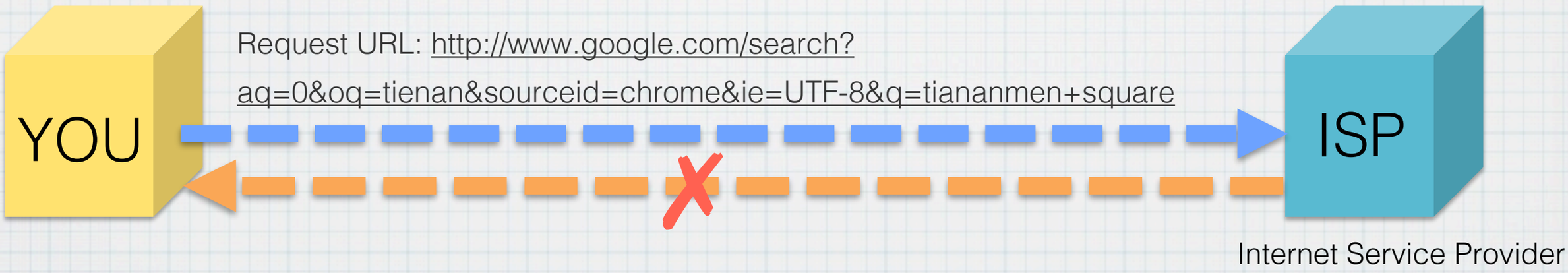
URL Filtering & Packet Filtering

The Chinese government will also examine the content of the URL that a request solicitor initiates a request with as well as the data they send inside of that request. These techniques are called URL filtering and packet filtering respectively.

URL Filtering

URL stands for Uniform Resource Locator. URL filters examine and make routing decisions based on the text in the URL.





A user initiates a Google search for “Tiananmen Square”. This creates a request URL with “tiananmen+square” in the URL, which is intercepted by the Chinese government and dropped.

Packet filtering.

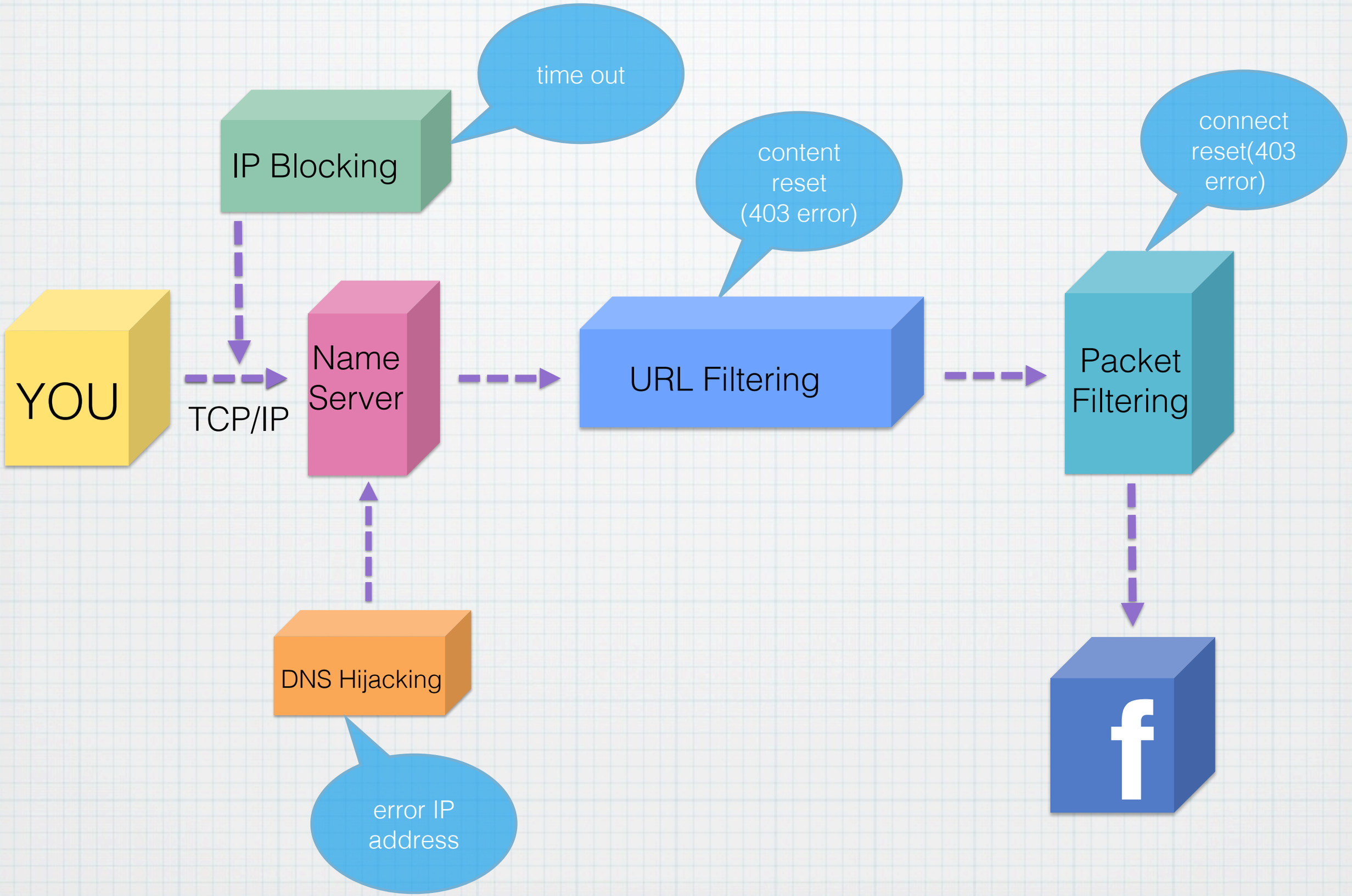
It examines the individual packets of data that are transferred between the client and target computers. Packets can be filtered based on content. A packet containing the search term “Falun Gong” could be intercepted and blocked or redirected.

In this case, a user navigates to a URL that doesn’t have any obviously discernible characteristic that ought to become blocked. However, the website itself contains information about Falun Gong: a system of beliefs and religious movement in China. The firewall, intercepting such information, would identify Falun Gong in the data and block further transmission.

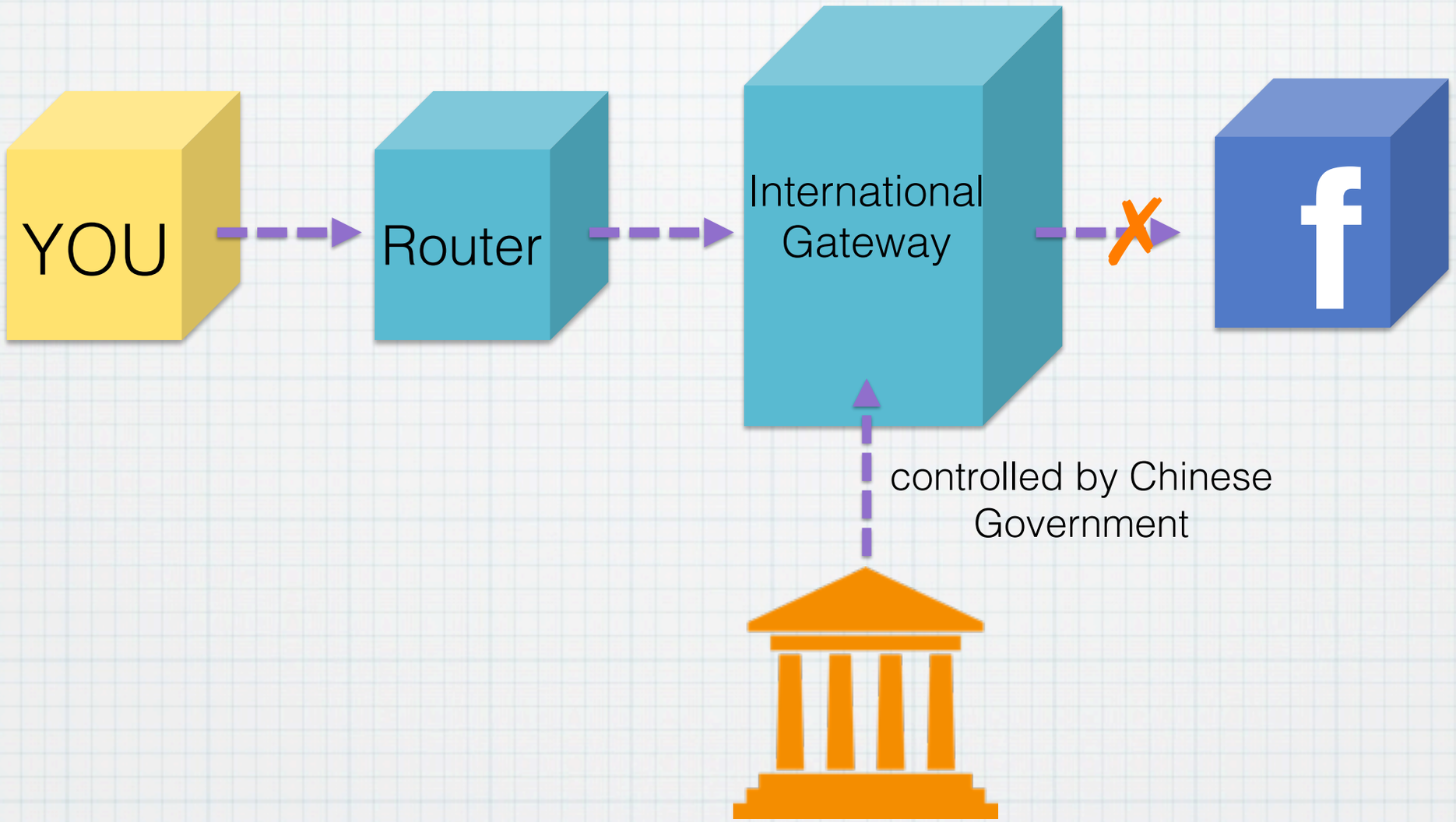
One way to avoid URL Filtering and Packet filtering to use HTTPS.
HTTPS is a communications protocol for secure communication over a computer network.

HTTPS not only encrypts the contents of a web page, but also the specific URL of the page being requested. Unless you have access to the private keys for a given site, it is difficult for Chinese government to determine exactly which URL within a site is being accessed in a secure browsing session.

Conclusion: when a user visit a website in China, the Great Firewall will do four things (IP Blocking, DNS Hijacking, URL Filter and Packet Filtering) to censor the website.



Chinese firewall is actually a network of its own, where is the government sitting between the client and the server. It is a network of service and inter-connection providers that are closely regulated by the Chinese government. International connections for all China's networks pass through proxy servers at official international gateways.



Because many enormous sites still use insecure HTTP rather than HTTPS. HTTP allows the Great Firewall to look those site, filter them, even modify them. In fact, without HTTPS, anyone sitting between the web server and the end user can modify content arbitrarily.

The hardware of Chinese fire wall are deployed on the international gateway and local Internet centers of China's major ISPs (Internet Service Provider, smaller ISPs are sharing the same gateway with major ISPs).

Till now, no one actually knows the physical position of GFW's hardware devices due to national security. However, there were projects trying to figure out the number and the position of the devices, the most recent one is called mongol.py: http://m.letscorp.net/archives/42652. The image below shows their research result.

The original reason they did this

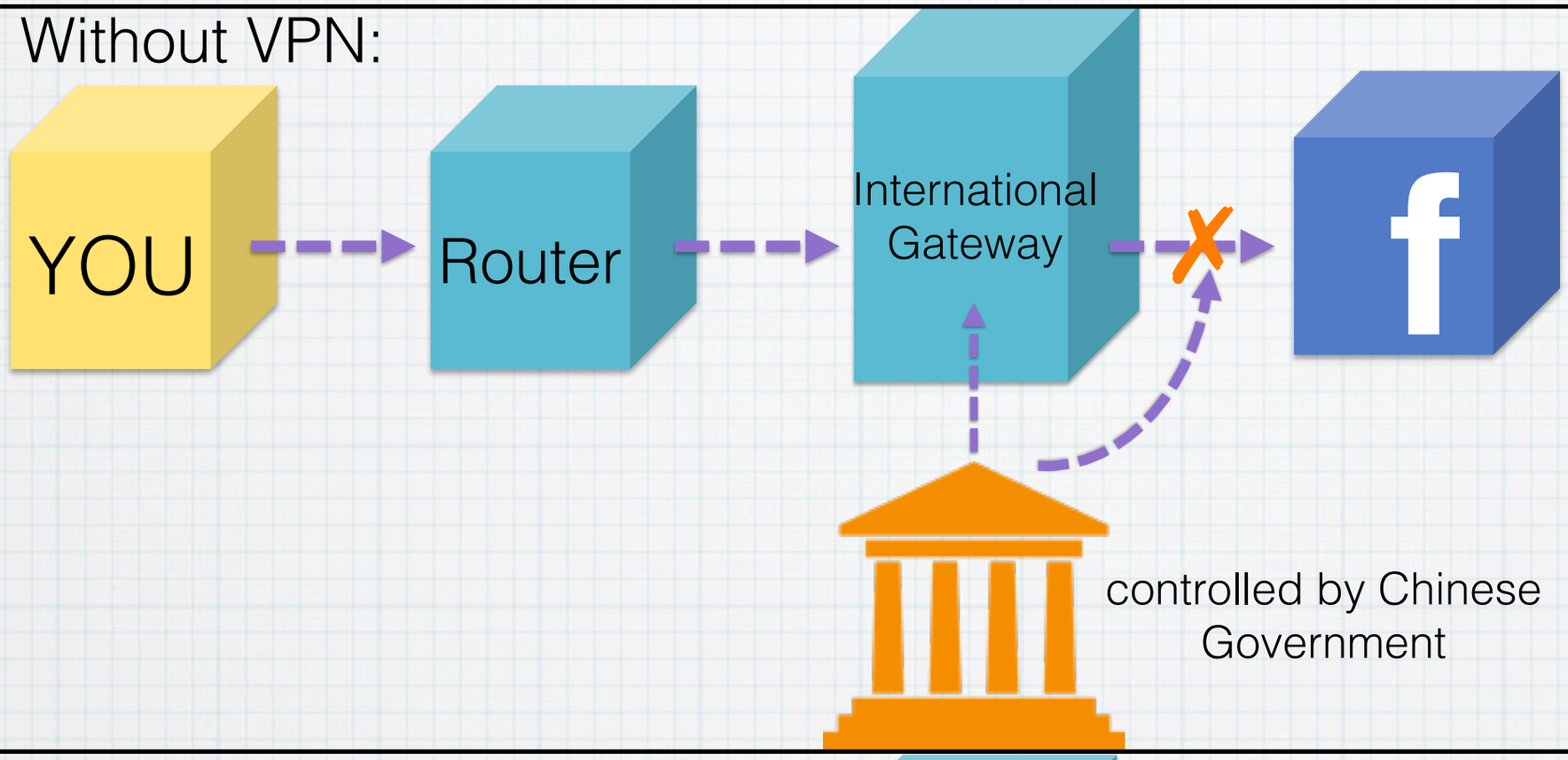
From the first linking of China to the global Internet in 1994, central authorities have consistently sought to control China's Internet connections. Heavily restricting international connectivity was a key principle in China's nascent Internet security strategy.

China's Internet regulation are guided by the principle of "guarded openness" - seeking to preserve the economic benefits of openness to global information, while guarding against foreign economic domination and the use of the Internet by domestic or foreign group to coordinate anti-regime activity.

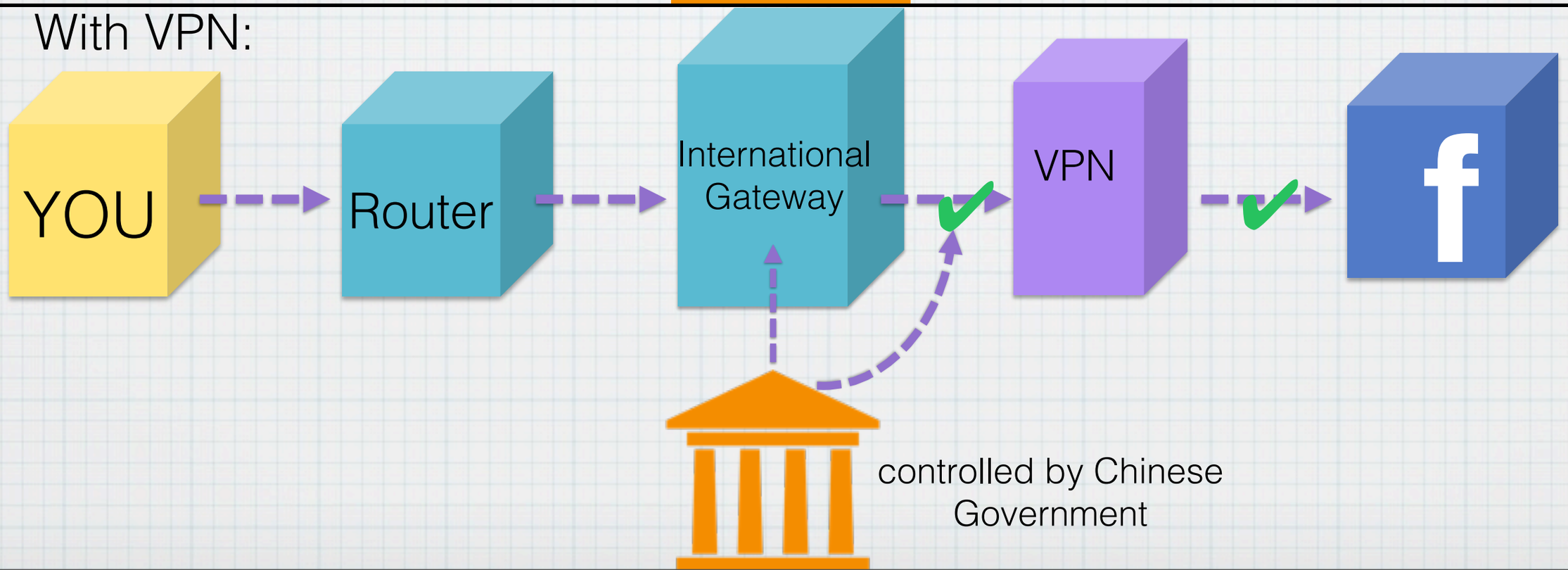
Originally, the firewall would modulate the pace of China's opening up to the world through electronic interaction. The government would decide at what rate to expand the connections and could theoretically shut them down in a social emergency.

There are many ways to bypass the firewall. One of the common ways is to use VPN. VPN refers to Virtual Private Network, which is a server you route your internet usage through. A VPN makes you appear as if you are in the country where the VPN server is located.

Without VPN:



With VPN:



References:

1. **How the Great Firewall of China Works [INFOGRAPHIC]**

   https://www.techinasia.com/great-firewall-china-works-infographic/

2. **Golden Shield Project**

   http://en.wikipedia.org/wiki/Golden_Shield_Project

3. **The Great Firewall: a technical perspective**

   http://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/great-firewall-technical-perspective/index.html

4. **The Great Firewall: How China Polices Internet Traffic**

   http://certmag.com/the-great-firewall-how-china-polices-internet-traffic/

5. **Who Has the Most Web Servers?**

   http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the-most-web-servers/

6. **The Great Firewall of China**

   http://campus.murraystate.edu/academic/faculty/wlyle/540/2013/Bu.pdf

7. **China's Golden Shield: Corporations and the Development of Surveillance**

   http://www.freerepublic.com/focus/f-news/582542/posts

8. **Virtual Private Networks**

   https://www.dropbox.com/s/wcz8n65pe9tafjp/VirtualPrivateNetworks.pdf